**大网区块链**

**数字身份和证书**

**崔建军博士 和Wolfgang Blumental**

**cui@inasset.de**

**微信：cui8161188**

摘要

 大网区块链提供了一种自我为中心身份解决方案，以推动第四次工业革命和物联网，为人，机器，算法和其他非人类实体带来安全的身份。 作为解决方案，它提供信息而无需透露详细信息。身份也是私密的和安全的。

大网区块链自我为中心身份是一种自我主权身份解决方案，该身份由政府授权或第三方发布，然后转移给用户，由用户自我管理。

大网区块链具有近实时确认，每秒百万交易，无许可和自我为中心公共区块链。

1.为什么数字身份证很重要？

身份证是每个社会的基石，数字化身份证是纸质身份证数字化形式。纸版身份证的基础是国家发行，个人持有使用。验证使用时是去中心化的。类似于纸版货币。检测身份不需要国家验证。

2.为什么至今没有可行的数字化身份证？

各个国家投入大量资源都没有解决数字化身份证使用的问题。数字化后是任何内容都可以简单的复制。只有区块链解决了数字不可复制性。所以有数字化货币。只有大网区块链解决了数字化身份证。实现了实人认证个人持有数字身份证。

3.数字身份证对大网有什么价值？

做为基础设施， 全世界每个人都成为自然而然的大网区块链用户！

数字化身份证减少费用，可以自动化验证，在银行开账户，申请手机号等需要身份证场景都可以使用。打车，乘火车及飞机都可以使用数字化身份证自动验证，加快安全检测。
打车应用，乘客打开大网钱包显示出身份证信息，包括图片，司机和乘客可以验证相互的身份保证安全。并且可以自动化。

数字化身份证一次验证，每个网站都可以应用。

目录

[数字身份 3](#__RefHeading___Toc446_2117361767)

[大网区块链 6](#__RefHeading___Toc448_2117361767)

 [政府作为身份颁发者 7](#__RefHeading___Toc450_2117361767)

 [服务提供商的用例 7](#__RefHeading___Toc293_1982971468)

[创建域名 7](#__RefHeading___Toc299_1982971468)

[创建数字身份证 9](#__RefHeading___Toc301_1982971468)

[撤销通证 14](#__RefHeading___Toc517_1743382299)

[大网区块链数字身份证和自动化验证 15](#__RefHeading___Toc519_1743382299)

#

# 数字身份

数字身份是纸质身份的数字形式。

身份解决方案包括个人和组织内用于识别，认证和授权某人访问该组织或其他关联组织中的服务或系统的过程和技术。数字身份是对纸质身份的替代，包括例如出生证明，身份证，护照或驾驶执照。数字身份需要随时随地可移植且可验证，也必须是私密和安全。

当前身份系统的问题：

政府：部门与政府之间缺乏互操作性。增加流程的时间和成本。

医疗保健：医疗保健领域（医院，诊所，保险公司，医生，药房等）的参与者之间缺乏互操作性，导致医疗保健效率低下，患者护理延误和沮丧。

教育：据估计，仅在美国，每年就售出二十万份假学术证书。难以验证这些凭证的真实性会导致雇用不合格的专业人员，对大学和雇用公司造成品牌损害。

银行业务：对登录详细信息（例如密码）的需求降低了用户银行业务的安全性。

一般业务：需要存储客户和员工的个人数据是公司的责任之一。

违反GDPR的行为（例如英国航空公司的案子），或者仅仅是由于客户信任损失和对组织品牌的间接损害，可能会导致个人数据泄露，从而处以巨额罚款。

# 大网区块链

大网 (大网)是新一代的区块链。大网 (大网)通过集成家谱与马尔可夫链蒙特卡洛(MCMC）扩展了区块链技术。因此，BITCOIN和以太坊在大网 (大网)中是特例。

通过使用大数据技术及其可并行化架构，大网是传统区块链的后续产品，可以满足具有重要经济意义的关键应用。

大网 (大网)是一个去中心化的加密货币，支付，交易，供应链和电子商务平台，具有以下优势：

* 近实时确认，分布式工作证明,
* 无限的可扩展性,
* 去中心化交易所，
* 去中心化供应链和电子商务
* 智能合约,
* 易于使用,
* 免费, 无许可，无信任，
* 量子安全。

大网是客户端和服务器体系结构。与任何基于工作证明PoW的系统相比，大网 所需的功耗与比特币相同。

但是，通过比较每秒交易量（TPS），例如比特币中的10 TPS或以太坊中的200 TPS，大网 (大网)在集群中具有10个服务器节点可以在相同的功耗下达到100万TPS。大数据和区块链并行化是以可承受的成本获得大量TPS的唯一解决方案。



#   政府作为身份颁发者

1.政府在大网区块链中创建一个域，例如id.gov

2.政府为身份证创建通证，通证名称必须是用户的公钥。 数据将用政府的公钥保存为通证的加密数据。

3.政府将通证转移到用户帐户，并使用用户公共密钥对身份数据进行加密。

4.政府可以撤销通证，应用程序可以验证数字身份。

5.用户可以为新的公钥请求新的数字身份。

#  服务提供商的用例

1.创建一个域id.idnow.de

2.检查纸质身份证，然后为身份证创建通证，通证名称应为用户的公钥。 数据将保存为使用公钥加密的数据。

3.将通证传输到用户帐户，使用用户公共密钥加密数据。

4.可以撤销通证，应用程序可以验证数字标识。

5.用户可以为新的公钥请求新的数字身份。

# 创建域名

大网区块链具有类似于互联网域名的分布式域名服务。 系统可创建顶级域名gov，com等。顶级域名的所有者可以创建具有多重签名的子域名。 域名是唯一的，并受多重签名保护。所有通证都属于一个域名。

打开创建审核机构并发布



# 创建数字身份证

身份将由域所有者组创建。 身份是在给定的公钥上颁发的，并且仅对此公钥有效。 身份数据由用户公共密钥加密，并具有颁发者的签名以验证身份。 所有身份数据均已加密。将数字身份证给用户。

身份通证可以通过可以使用公共检查此地址公共密钥是否具有通证, 全名为 HashOfIdentity@id.gov的通证。

实人认证流程

https://bigtangle.oss-cn-beijing.aliyuncs.com/app/identity\_verify.apk下载实人认证

APP，并安装后运行该实人认证APP。

输入用户名、密码及大网钱包的密码（如果已加密钱包）后，点击“实人认证”按钮开始进入实人认证流程。





点击“同意”按钮后，进入人脸认证和身份证照片上传操作页面。







必须点击“返回”按钮完成签名。

# 撤销身份通证

身份由域所有者组创建。域所有者可以撤销身份通证。

创建域名: cancel.id.gov

撤销通证: HashOfIdentity@cancel.id.gov

撤销通证, 用户可以为新的公钥请求新的数字身份。

# 大网区块链数字身份证和自动化验证

自动化验证必须验证两个条件:

a. 数字身份存在, 并且有效

b. 钱包里对应的私钥, 验证钱包持有数字身份

自动化验证流程:

1) 用户扫描验证器端二维码。

2) 验证端(服务器)查询数字身份存在, 并且有效,验证钱包里对应的私钥。

1) 验证器端生成二维码页面生成一个带有URL两个参数的二维码，以JSON格式存放

JSON：{

“url”: “[https://m.bigtangle.xyz/public/loginscan](https://m.bigtangle.xyz/public/qrscan)”，

}

2) 钱包APP里扫描二维码页面，将其中的url接收下来，

然后把钱包里的其中数字身份公钥地址publickey=tokenid和及状态标志传给url，

服务器端用publickey将useraccesstoken加密，并将加密后的信息解码为字符串useraccesstoken传回手机APP里，

手机APP里用刚才publickey对应的privatekey解密这条字符串消息useraccesstoken，

如果解密成功，再次调用这个url，并将publickey、useraccesstoken。

服务器验证useraccesstoken成功。